

Remarks

Applicants would first like to thank the examiner for withdrawing the double patenting rejection. Claims 1-39 are currently pending.

1. Response to § 112, Second Paragraph Rejections

The Examiner rejected claim 25 under 35 U.S.C. § 112, second paragraph for lack of antecedent basis. Applicants have amended this claim to remove the limitation of the “first protocol”, rendering the rejection moot. Although the scope of claim 25 was increased, no new matter was added.

2. Response to §102(e) rejections:

The Examiner rejected claims 1-27 as anticipated by Ylonen (U.S. Patent No. 6,438,612) under 35 U.S.C. § 102(e). Applicants submit that Ylonen does not disclose all the elements of Applicants’ claimed invention. In addition, applicants have enclosed with the present response a Declaration in compliance with 37 CFR §1.131 and supporting documentation to show that the presently claimed invention antedates Ylonen (and Danieli).

As an initial matter, it is important to keep in mind that all of the pending claims recite distributed network address translation (DNAT) with security. For example, Claim 1 of the present application recites “requesting ... one or more locally unique security values from a second network device ... for distributed network address translation with security.”

The present invention can be useful for solving security problems associated with network address translation. This was noted in the background section of the present application.

There are several problems associated with using current versions of NAT when security is required and the IPSEC protocol is used. Current versions of NAT violate certain specific principles of the IPSEC protocol that allow establishment and maintenance of secure end-to-end connections of an IP network.

A NAT router typically needs to modify an IP packet (e.g., network ports, etc.). However, once an IP packet is protected by IPSEC, it must not be modified anywhere along a path from an IPSEC source to an IPSEC destination. Most NAT routers violate IPSEC by modifying, or attempting to modify individual IP packets.

Even if a NAT router does not modify data packets it forwards, it must be able to read network port numbers (e.g., TCP, UDP, etc.) in the data packets. If certain IPSEC features are used (e.g., Encapsulated Security Payload ("ESP")), the network port numbers are encrypted, so the NAT router typically will not be able to use the network ports for NAT mapping.

Local host network devices on a Local Area Network ("LAN") that use NAT typically possess only local, non-unique IP addresses. The local non-unique IP addresses do not comprise a name space that is suitable for binding an encryption key (e.g., a public key) to a unique entity. Without this unique binding, it is not possible to provide necessary authentication for establishment of Security Associations. Without authentication, an endpoint of a connection cannot be certain of the identity of another endpoint, and thus cannot establish a secure and trusted connection.

Patent Application, p. 5, ln. 19 to p. 8, ln. 9.

DNAT allows a single routable IP address may be multiplexed among several hosts on a local stub network, none of which have a globally routable IP address. Thus, for example, DNAT is useful for extending the lifetime of IP-4 systems. Additionally, DNAT allows routers to perform the required address mapping without modifying the contents of the routed packets. (i.e., TCP/UDP header, or payload). Further, the present invention provides for distributed network address translation using Internet Protocol

security in a way that does not significantly increase a burden on the routers or other network devices that provides network address translation.

Ylonen does not teach DNAT. In fact, Ylonen does not teach network translation in any form. In contrast with the each claim of the present application, Ylonen simply teaches a secure communication tunnel established between two virtual routers on two separate virtual networks with IPSEC protocols utilizing IKE SA, or ESP transforms. *See* Ylonen, col. 4 lines 39-67 and col. 5 lines 1-4. Because Ylonen does not provide any teachings as to network address translation or DNAT, it cannot anticipate the presently claimed invention.

Further, Ylonen lacks several features of the presently claimed invention. For example, Ylonen does not disclose two network devices interoperating on the same computer network (independent claims 1, 9, 14, 20, 28, 34, and 36). Likewise, Ylonen does not teach storing locally unique security values on the first network device – that is the local network device (independent claims 1 and 9).

The differences between Ylonen and the present invention continue. For example, contrary to independent claims 1, 9, 34, and 36 Ylonen fails to disclose requesting or receiving “locally unique security values” from a second network device on the same computer network to uniquely identify the first network device.¹

Next, claims 3, 11, 31, and 37 contain the limitation of the second network device being a distributed network address translation (DNAT) router. A DNAT router is used to allocate “locally unique security values that are used as the Internet Protocol security protocol security parameters indexes. A router used for distributed network address

¹ Claims 7, 20, 28, 34, and 36 refer to “locally unique ports” which are likewise not disclosed by Ylonen.

translation is also used as a local certificate authority that may vouch for identities of local network devices, allowing local network devices to bind a public key to a security name space.” Patent Application, Summary of Invention.

As shown by the examiner, Ylonen does disclose a router. However, Ylonen’s router is not given any of the functionality associated with the above described DNAT router. “[A] router is arranged to process packets both to itself and packets destined to other computer devices of the network. Routers may further be sub-classified; some sub-classes are for example IP routers (Internet Protocol) and access routers.” Ylonen, Col. 1, lines 17-22 (section cited by Examiner). Ylonen simply does not disclose DNAT routers of claims 3, 11, 31, and 37.

Ylonen does not teach each and every element in any of the claims. Thus, its use as an anticipatory reference is improper and must be withdrawn.

3. Response to 103(a) rejections:

The Examiner rejected claims 28-39 as obvious by Ylonen (U.S. Patent No. 6,438,612) in view of Danieli (U.S. Patent No. 6,510,513) under 35 U.S.C. § 103(a). According to M.P.E.P. § 2143, in order to establish a prima facie case of obviousness of a claimed invention by applying a combination of references, the proposed combination must teach or suggest all of the elements of the claimed invention. Applicants submit that the combination proposed by the Examiner does not teach or suggest all of the elements of Applicants' claimed invention and, therefore, that a prima facie case of obviousness of Applicants' claims does not exist.

As discussed DNAT forms an element of each of claims 28-39. Yet, neither Ylonen nor Danieli teach or disclose any aspect of DNAT. Ylonen provides a specific

method for tunnelling data between virtual routers while Danieli provides a Microsoft version of electronic security certificates. These are simply not applicable to the presently claimed method of distributed network address translation with security.

Therefore, the use of these two references is improper and the rejection of the present claims under §103 must be withdrawn.

4. Declaration of Antedate the References:

The Examiner asserts a Rejection of claims 1-39 as either anticipated by Ylonen (claims 1-27) or made obvious by Ylonen in view of Danieli (claims 28-39). Applicants submit a Declaration under 37 CFR § 1.131 establishing conception of the subject matter of the rejected claims prior to the effective date of either reference on which the rejections are based, as well as establishing that the subject matter of the rejected claims was diligently reduced to practice.

Applicants note that due to the unavailability of two of the named inventors,² Applicants' representative was unable to secure a fully executed Declaration. However, Applicants will secure and promptly submit an executed declaration containing signatures of all four named inventors.

Applicants contend that because the declaration sufficiently establishes the conception of the subject matter of the claims prior to the effective date of Ylonen and Danieli, and further, establishes that the subject matter of the rejected claims was diligently reduced to practice, the Declaration is sufficient to overcome the rejections of claims 1-39.

² One of the inventors is currently on an extended tour in India and has been unavailable to fully assist with the preparation of this response. He is expected to return by the end of August 2004.

Although under MPEP 715.07, averments made in a 37 CFR 1.131 declaration do not require corroboration, Applicants have provided a copy of their invention disclosure form. The invention disclosure form is attached to this paper as Exhibit A and fully demonstrates conception of the presently claimed invention. Of specific interest may be pages 13-15 of the invention disclosure form that describes using IPsec across a DNAT Network. Further, the present application is a continuation-in-part of U.S. Application No. 09/035,600 filed on March 5, 1998 (Now U.S. Patent No. 6,353,614).

As the Examiner will note, the invention disclosure form is a well drafted whitepaper. Like submitting the patent application, drafting the invention disclosure form shows diligence in reduction to practice. Likewise, at least four draft applications were written by outside counsel and reviewed by the inventors during the period of diligence. And, at least one other related application was filed during this critical period. The related application has now issued as U.S. Patent No. 6,697,354.

Under MPEP 2138.06, once the inventors provide a disclosure that is ready for patenting, "reasonable diligence is all that is required of the [prosecuting] attorney." Dr. Steven Lesavich, the attorney responsible for the initial prosecution of this case, worked reasonably hard on the application during the critical period. The attorney had a reasonable backlog of unrelated cases that were taken up in chronological order and carried out expeditiously. In addition, during this critical time, the attorney worked on related cases that contributed substantially to the ultimate preparation of the present application.

Accordingly, the rejections of pending claims 1-39 based on Ylonen or the combination of Ylonen and Danieli should be withdrawn.

Conclusion

In view of the foregoing, Applicants respectfully submit that all of the presently pending claims are now in condition for allowance, and Applicants respectfully request prompt favorable reconsideration.

Respectfully submitted,

Date:

July 26 - 2004

By:

DD Crouch

Dennis D. Crouch

Registration No. 55,091